MANUEL D'INSTALLATION D'UN PROXY

Squid, SquidGuard, Dansguardian

Dans ce guide on va détailler l'installation et la configuration d'une solution proxy antivirale en utilisant les outils ; squid, dansGuardian, squidguard et un antivirus Clamav sur un système d'exploitation linux debian lenny.

Agence Nationale de la Sécurité Informatique

Gestion de Gestion des versions de guide

Version	Date	Modification apportée
1.0	28/07/2010	Première version

Document Publique Document Interne

PLAN

1. présentation 3
2. Paramétrage du gestionnaire de package 4
3. Installation 5
   a. Installation de Webmin 5
   b. Installation de Squid 5
   c. Installation de SquidGuard 5
   d. Installation de DansGuardian 6
4. Configuration via webmin 7
   a. Squid 7
   b. SquidGuard 15
   c. DansGuardian 20
   d. Mise à jour de Dansguardian 23
   e. Configuration du client 24
5. Test de fonctionnement 24

1. PRESENTATION

Un serveur proxy est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les proxy sont notamment utilisés pour assurer les fonctions suivantes :

- mémoire cache
- la journalisation des requêtes (« logging »)
- la sécurité du réseau local
- le filtrage et l'anonymat

Notre serveur proxy va être composé de squid, squidguard et dansguardian

- Squid est un serveur proxy cache open source qui supporte les protocoles http, https, FTP et SSL. Il assure les fonctions de :

  - Cache : pour optimiser la bande passante
  - Contrôle des accès
  - Reverse proxy

- SquidGuard est un redirecteur de requêtes web qui utilise la librairie Berkeley Database. Il propose un filtrage puissant d'accès au web, en fonction de:

  - Groupes d'utilisateurs, définis de diverses manières.
  - Listes de domaines et d'URI qui serviront à définir soit des cibles autorisées, soit des cibles interdites,
  - Black listes de domaines et d'URI
  - Plages horaires

- DansGuardian est un système de contrôle de contenu. Il utilise plusieurs méthodes paramétrables pour déterminer si une page web doit être bloquée.

  - Il utilise ; un système de pondération qui détecte des mots interdits dans une page, et lui assigne un score en fonction de la gravité et du nombre de mots détectés. DansGuardian bloque alors les pages dont le score dépasse un certain seuil.

- Il peut également se fier à des listes noires d'URL telles que celle proposée par le site URLBlacklist.com, ou au code PICS d'une page web lorsqu'il est renseigné.

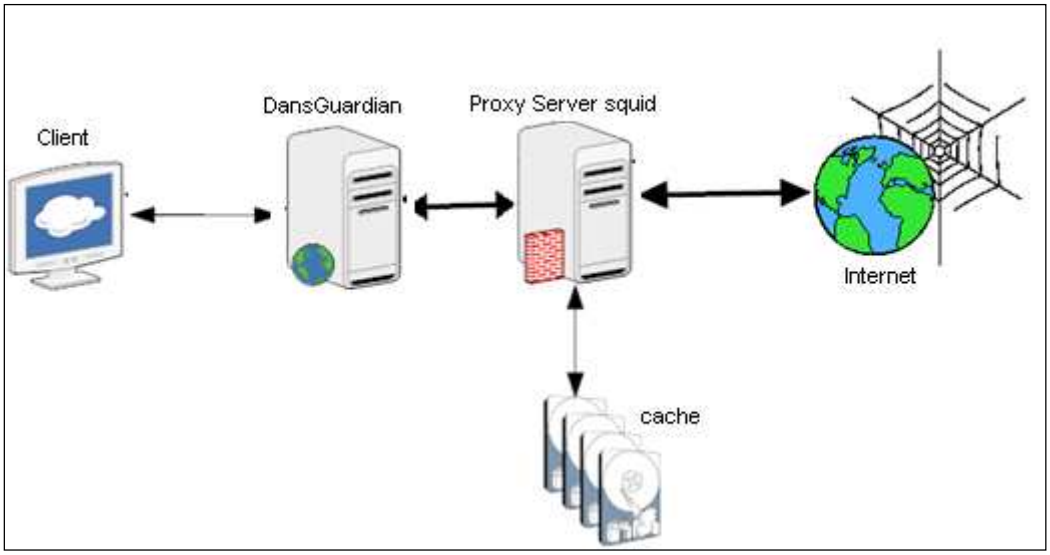


Fig1. Schéma de fonctionnement d'un proxy

2. PARAMETRAGE DU GESTIONNAIRE DE PACKAGE

- Changer le fichier /etc/apt/sources.list comme suit :

```
deb http://ftp.us.debian.org/debian lenny main

deb-src http://ftp.us.debian.org/debian lenny main

deb http://security.debian.org/ lenny/updates main

deb-src http://security.debian.org/ lenny/updates main

deb http://volatile.debian.org/debian-volatile lenny/volatile main

deb-src http://volatile.debian.org/debian-volatile lenny/volatile main
```

- Mettez à jour la liste des fichiers disponibles dans les dépôts APT présents dans le fichier de configuration /etc/apt/sources.list. puis mettez à jour tous les paquets installés vers les dernières versions

```
Apt-get update

Apt-get upgrade
```

3. INSTALLATION

a. Installation de Webmin

- Webmin est une interface web, qui permet d'administrer à distance notre serveur proxy (squid, squidguard et dansguardian).
- Télécharger webmin à partir de ce lien : http://prdownloads.sourceforge.net/webadmin/webmin-1.480.tar.gz
- Décompresser le :

```
Tar xzvf webmin-1.480.tar.gz

Cd webmin-1.480
```

- Installez-le :

```
./setup.sh
```

- Connexion à l'interface de webmin : https://adresse_de_host :10000

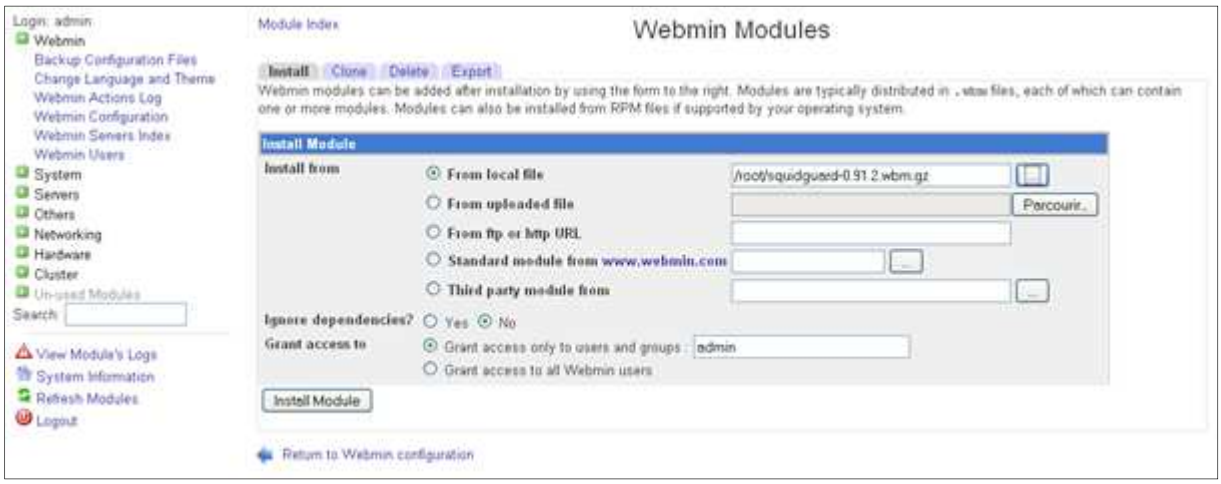
b. Installation de Squid

```
apt-get install squid
```

c. Installation de SquidGuard

```
apt-get install squidguard
```

- Téléchargez maintenant son module de webmin à partir de ce lien : http://www.niemueller.de/webmin/modules/squidguard/squidguard-0.91.2.wbm.gz
- Installez-le via webmin comme suit :



d. Installation de DansGuardian

```
apt-get install dansguardian
```

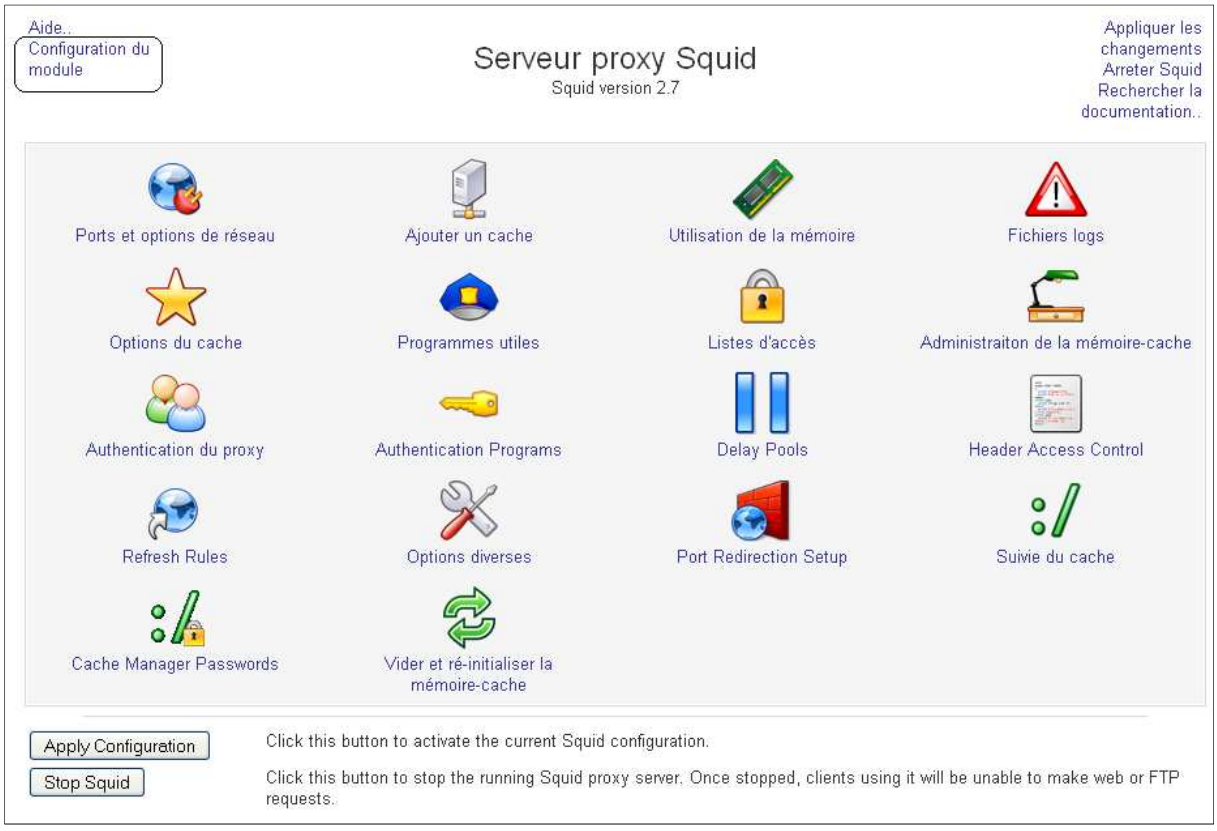
- Téléchargez maintenant son module de webmin à partir de ce lien : http://sourceforge.net/projects/dgwebminmodule/files/dgwebmin-devel/0.7.0beta1b/dgwebmin-0.7.0beta1b.wbm/downloadn
- Et faites de même que l'ajout du module de squidguard via webmin.

4. CONFIGURATION VIA WEBMIN

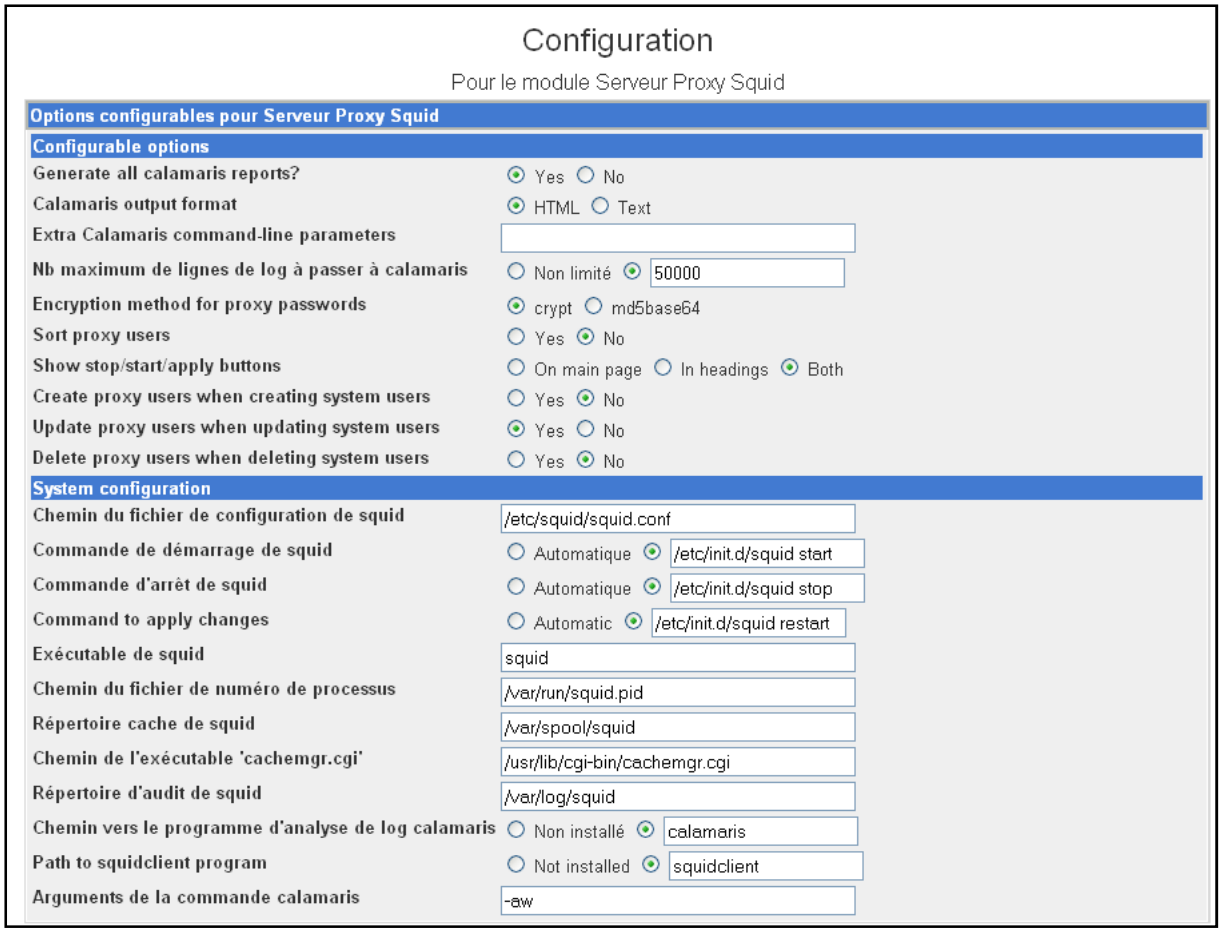
a. Squid

- **Configuration squid :**

- En haut de la page de « serveur proxy squid », cliquez sur « configuration du module ».

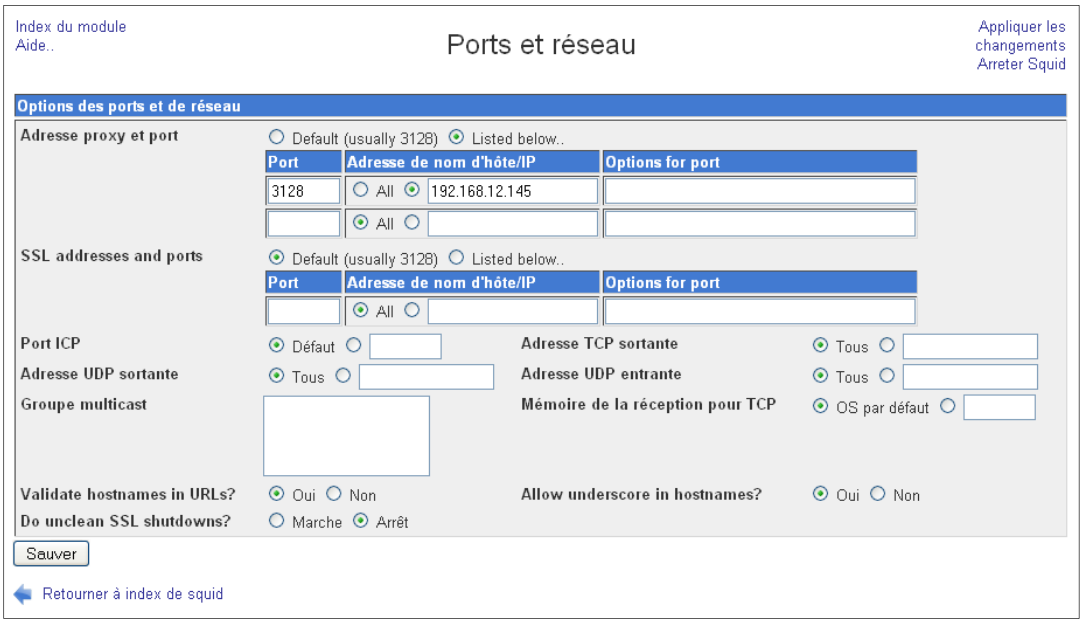


- Changez les commandes de démarrage, d'arrêt et de redémarrage comme suit, puis sauvegardez :



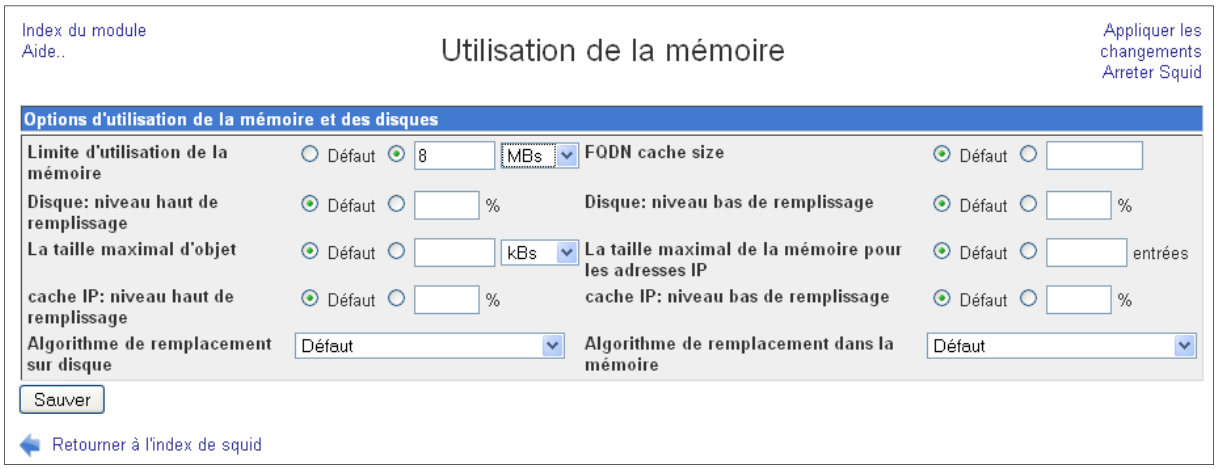
- **Port et adresse d'écoute :**

- Sous la catégorie serveur, cliquez sur serveur proxy squid, puis sur « port et options de réseau » et configurer le port et l'adresse de proxy.



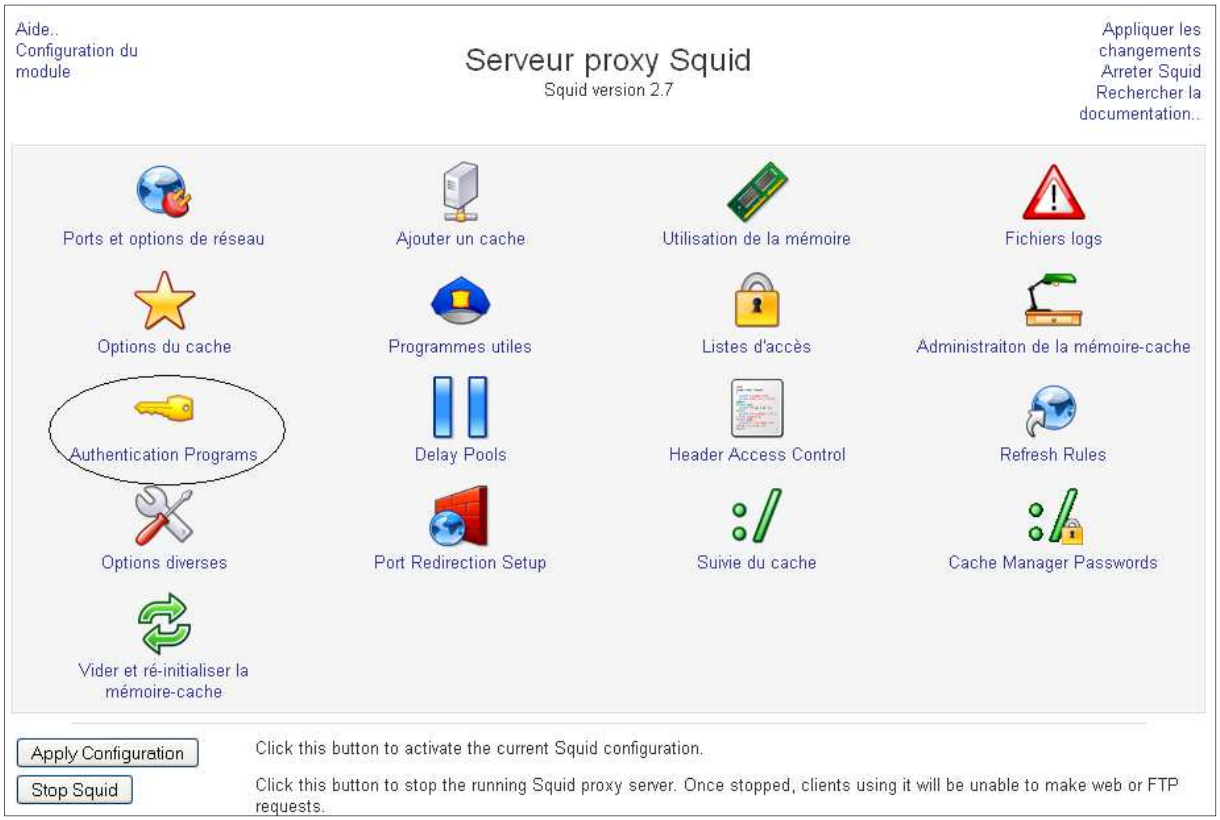
- **Utilisation de la mémoire :**

- Fixer l'utilisation de la mémoire (à 8 MB)

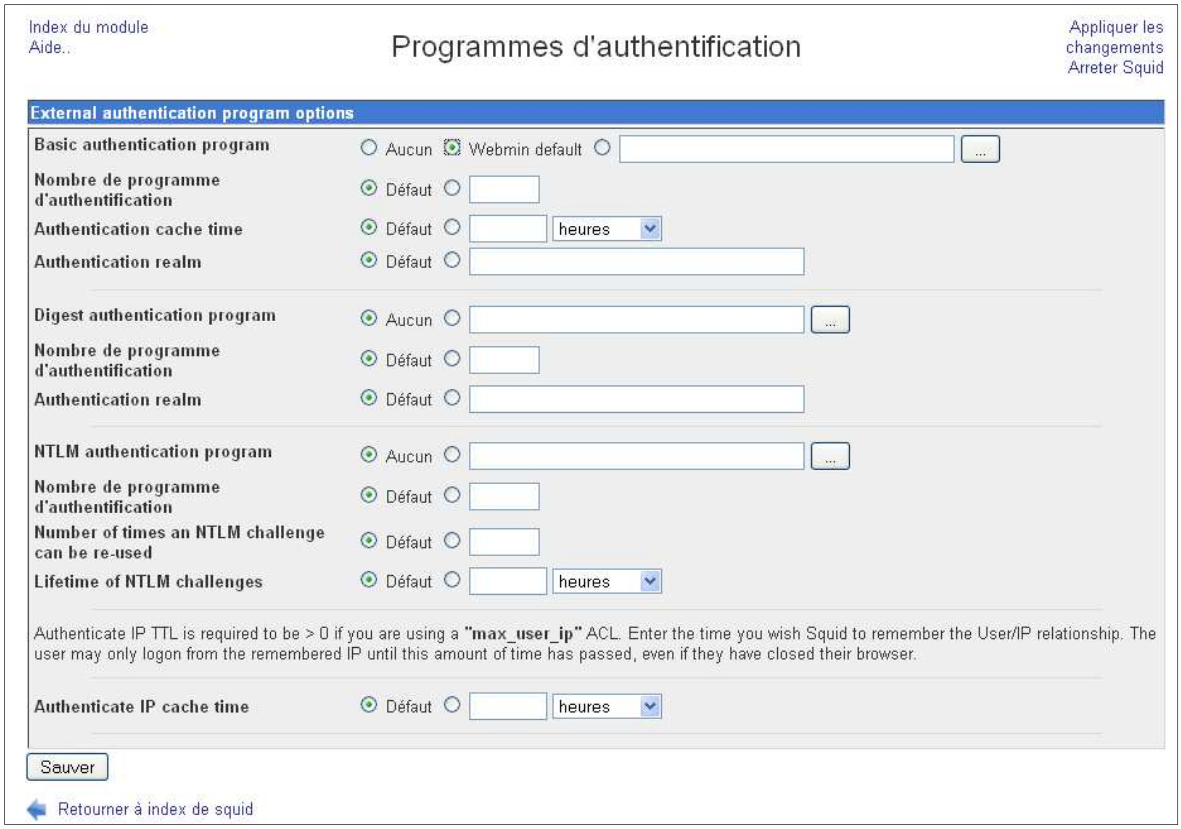


- **Ajouter l'authentification :**

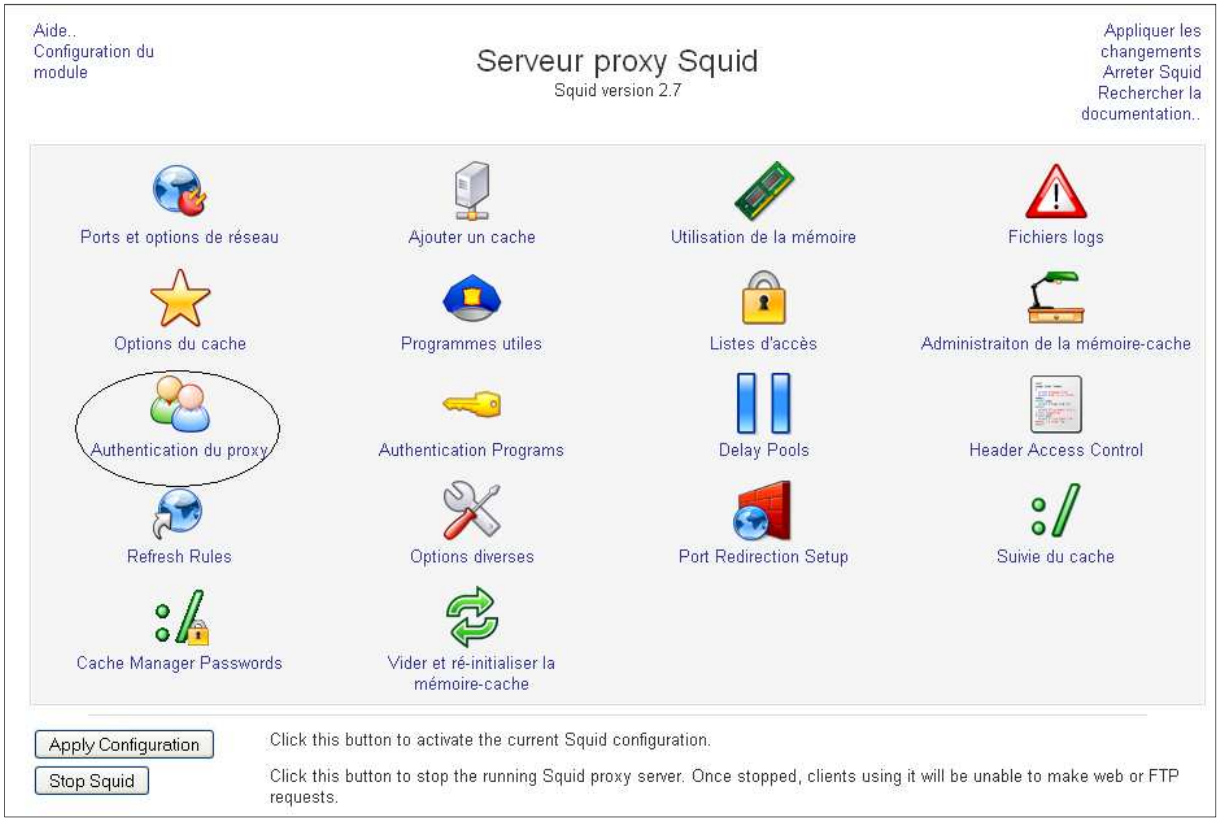
- Ouvrez l'onglet « Authentication Programs »



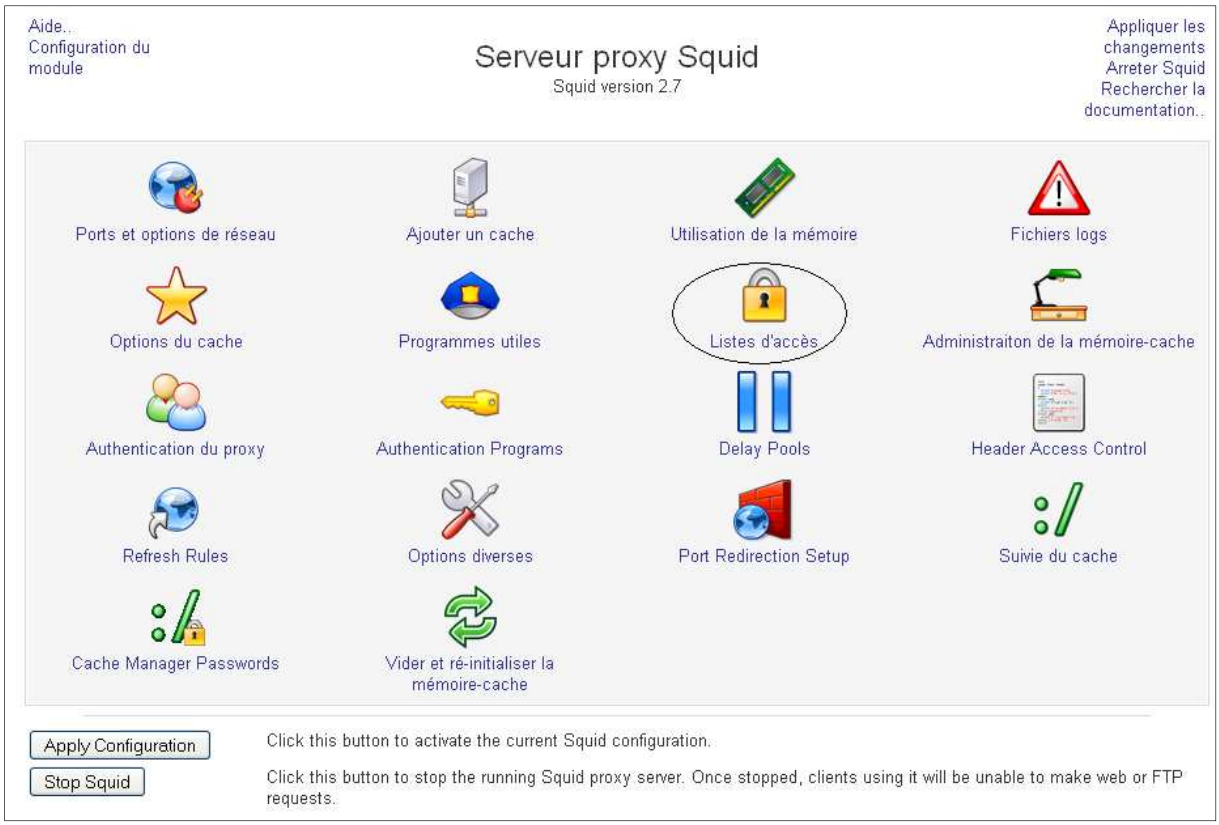
- Indiquer le programme d'authentification que vous allez utiliser. Sauvegarder et retourner à la page d'index.


Index du module
Aide..
Programmes d'authentification
Appliquer les changements
Arreter Squid
External authentication program options
Basic authentication program
Aucun
Webmin default
Nombre de programme d'authentification
Défaut
Authentication cache time
heures
Authentication realm
Digest authentication program
NTLM authentication program
Number of times an NTLM challenge can be re-used
Lifetime of NTLM challenges
Authenticate IP TTL is required to be > 0 if you are using a "max_user_ip" ACL. Enter the time you wish Squid to remember the User/IP relationship. The user may only logon from the remembered IP until this amount of time has passed, even if they have closed their browser.
Authenticate IP cache time
Sauver
Retourner à index de squid

- Il vous apparait un nouveau onglet nommé « Authentication du proxy », cliquer dedans et ajouter un nouveau utilisateur du proxy, puis cliquez sur créer.

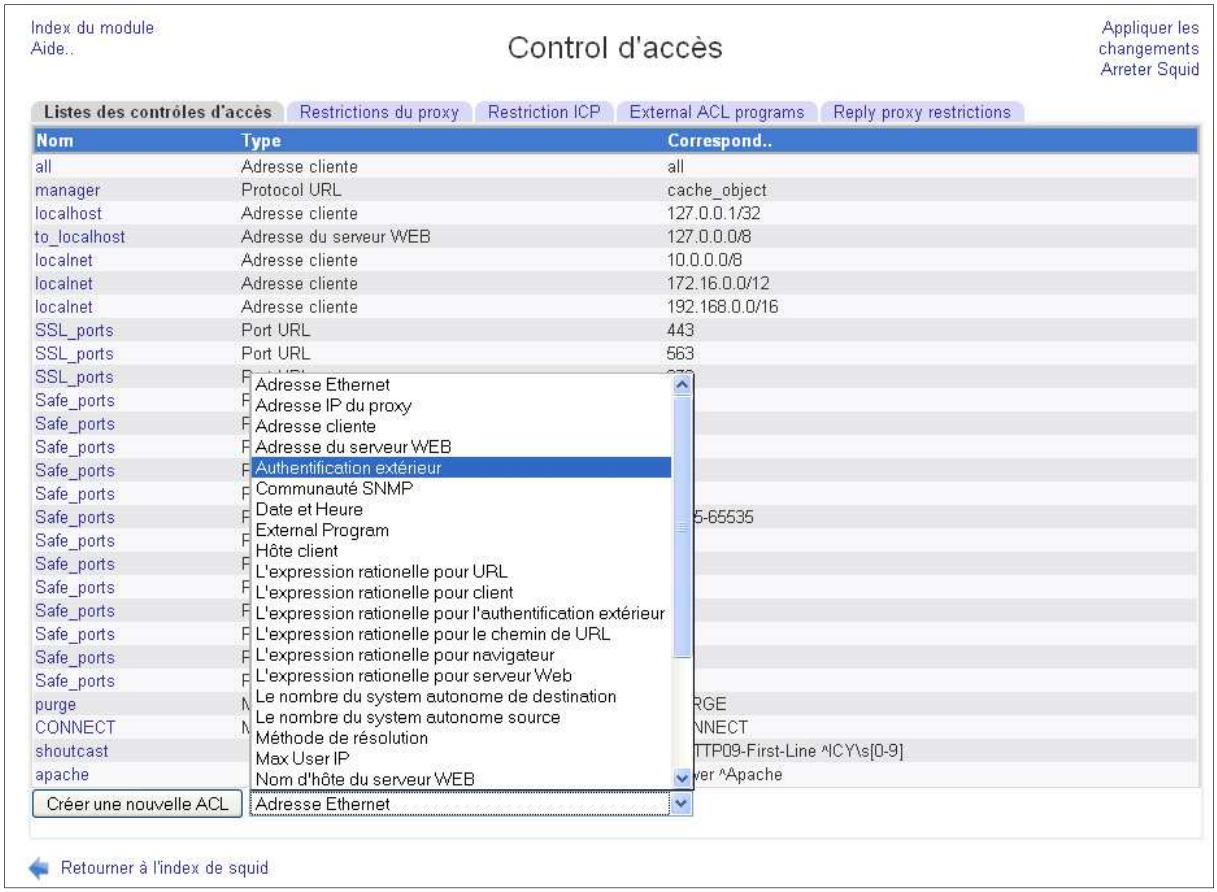


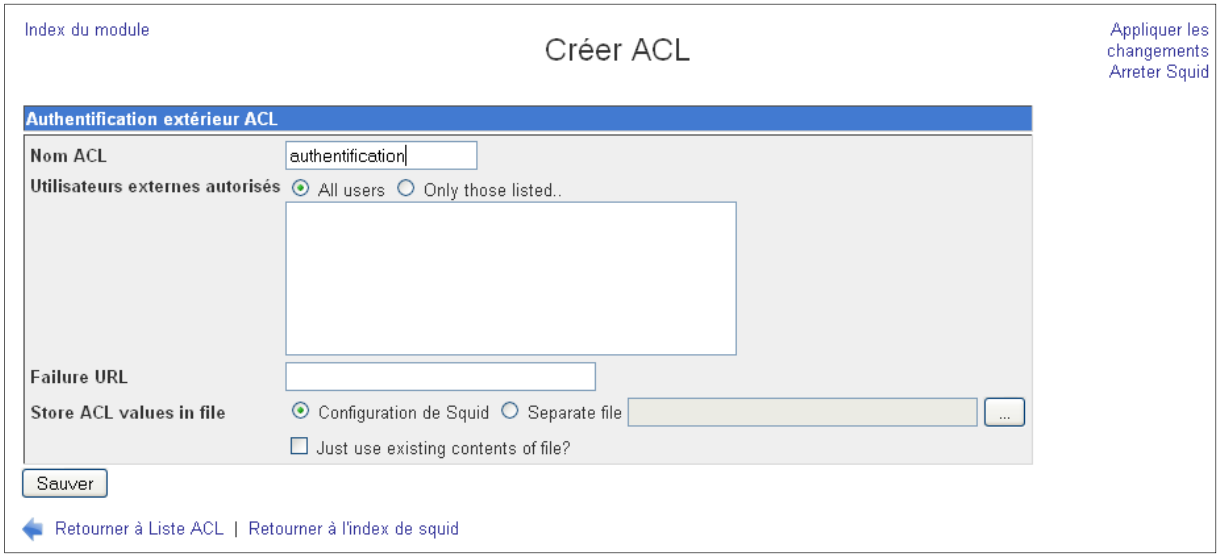
- **Mise en place des ACLs :**



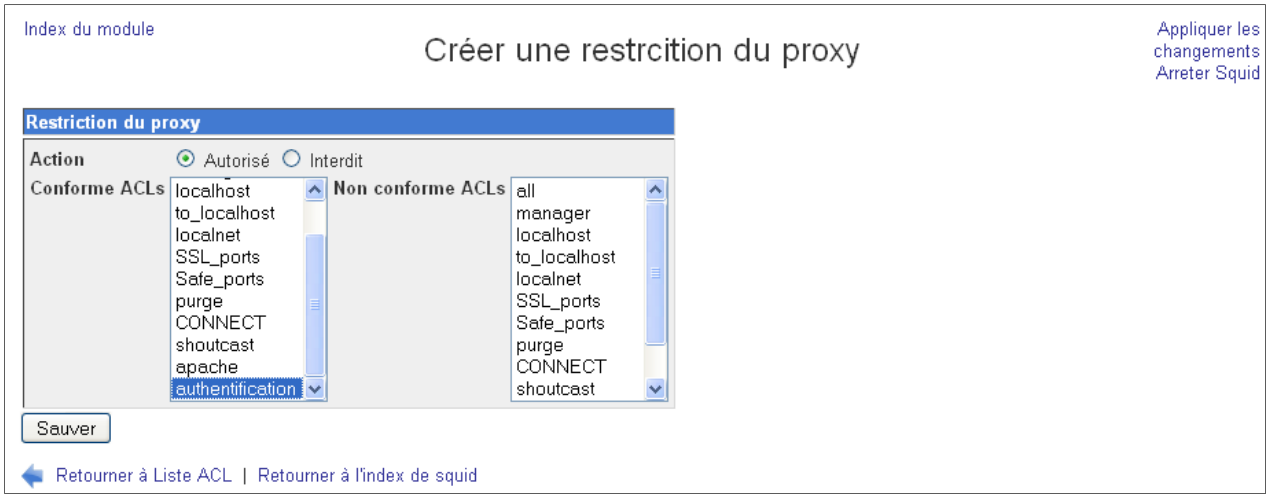
❖ Ajouter une première ACL pour l'authentification des utilisateurs :

- Créer une nouvelle ACL de type « Authentification extérieur » en lui donnant un nom signifiant.

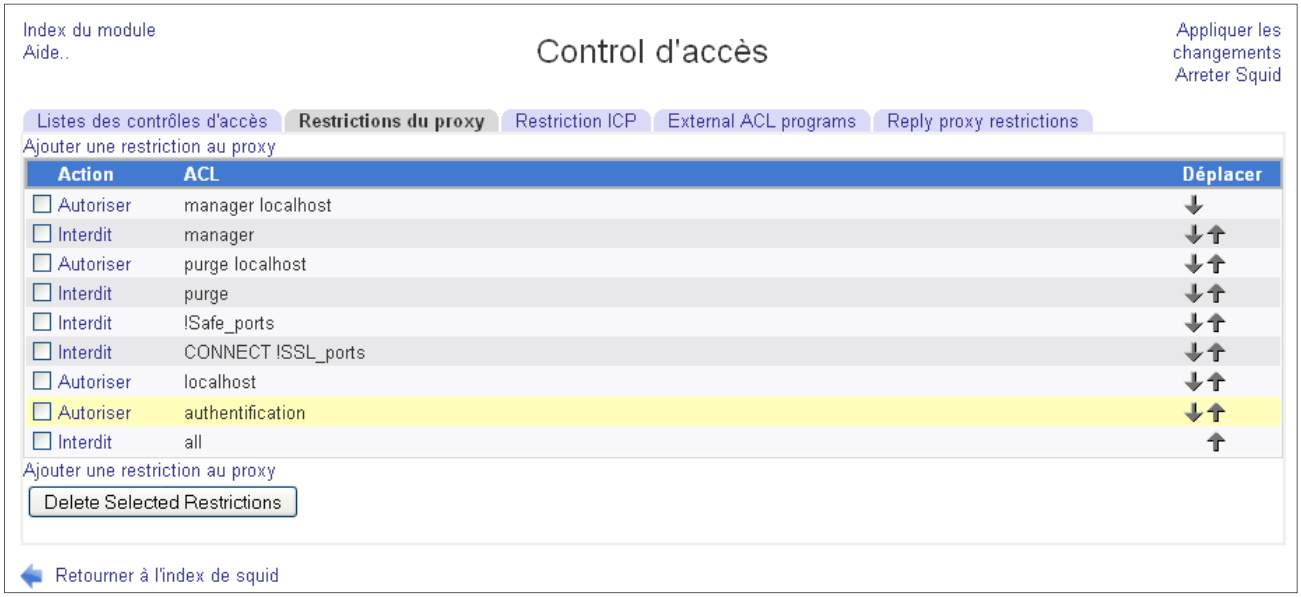




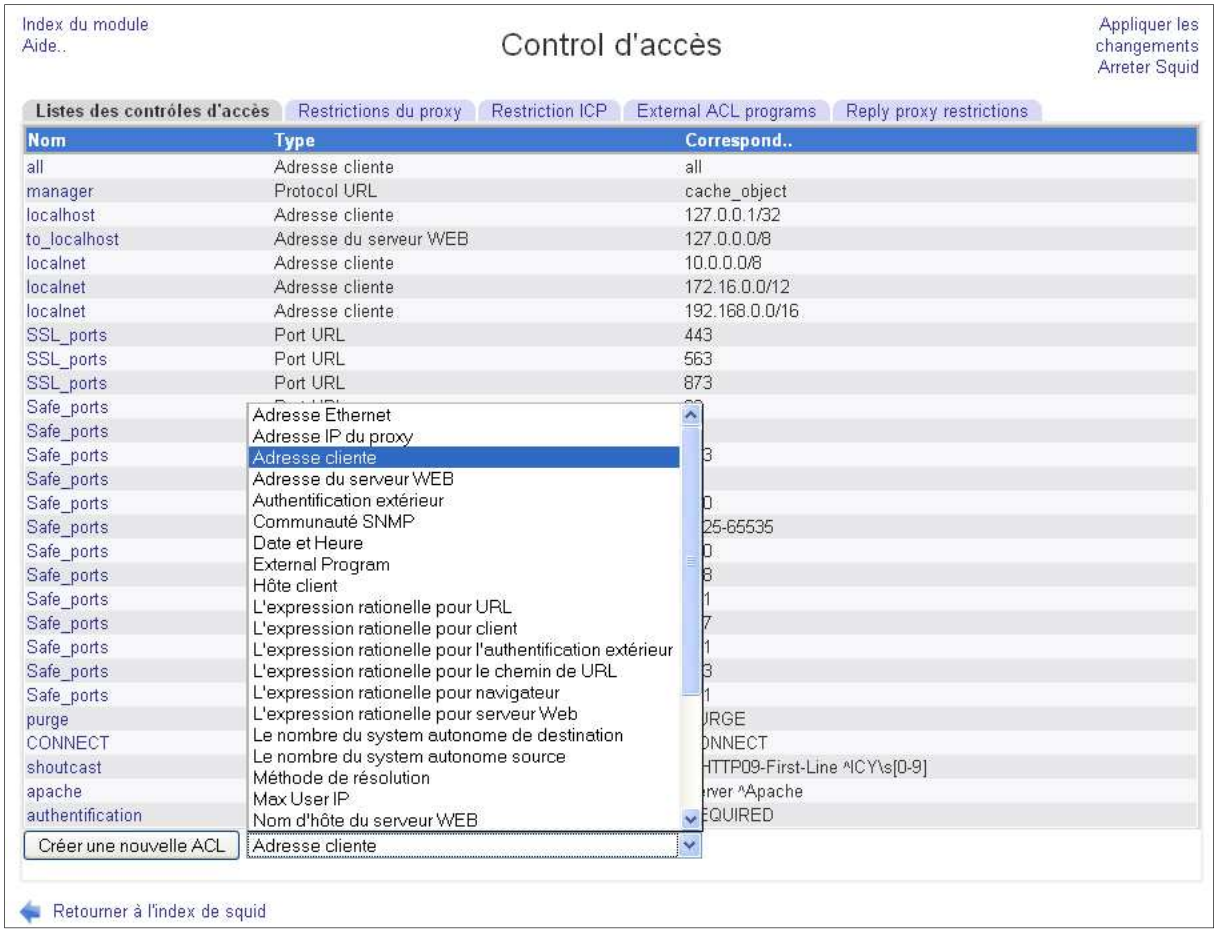
- Puis passer à l'onglet « Restrictions du proxy » et cliquer sur « ajouter une restriction au proxy ».
- Sélectionner le nom de votre ACL, et choisissez l'action «Autorisé». Sauvegardez



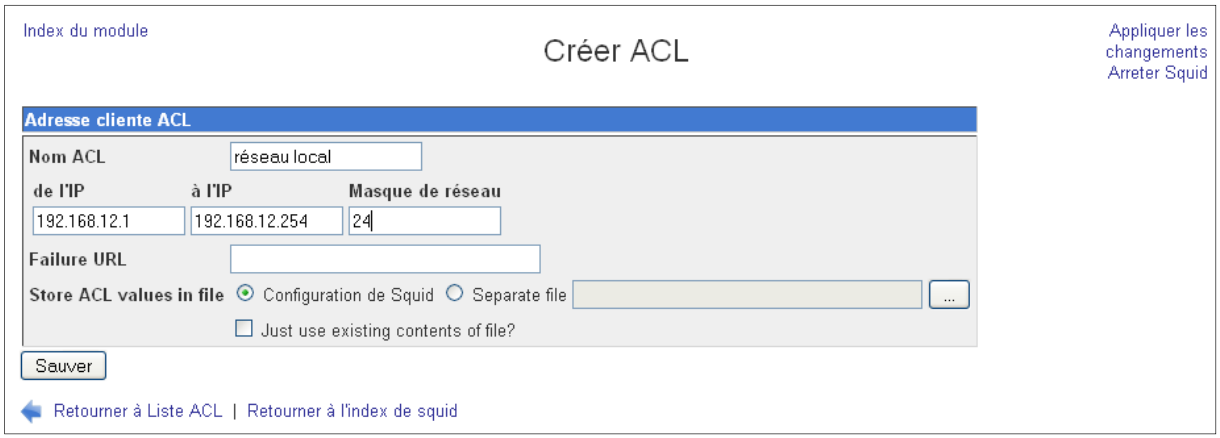
- Retournez à la liste des ACLs, et faire remonter la restriction que vous venez de créez juste au-dessus de la restriction « interdit all ». Parce que squid prends en compte l'ordre des ACLs.



❖ Ajouter une deuxième ACL pour l'accès d'adresse client :



- Créer une nouvelle ACL de type « Adresse cliente » en lui donnant un nom signifiant.



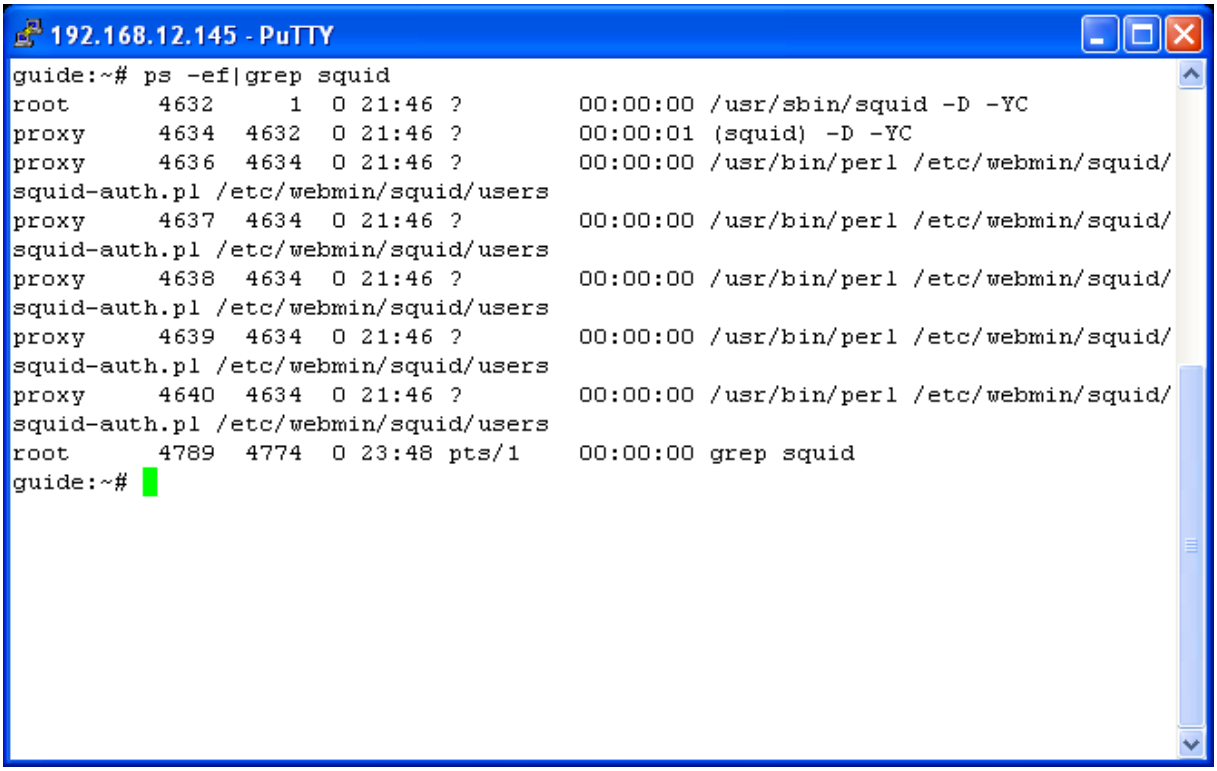
- De même que l'ACL précédente, ajoutez une restriction à cette ACL en lui donnant l'action «Autorisé».
- Et faire remonter la restriction que vous venez de créez juste au-dessus de la restriction « interdit all ».

- **Test de fonctionnement de squid :**

- Dans l'interface principale de squid, cliquez sur « Appliquez les changements » en haut de la page.
- Ensuite, vérifiez le bon fonctionnement de Squid en utilisant le Shell.

```
guide:~# /etc/init.d/squid status
squid is running.
```

Ou


192.168.12.145 - PuTTY
guide:~# ps -ef|grep squid
root 4632 1 0 21:46 ? 00:00:00 /usr/sbin/squid -D -YC
proxy 4634 4632 0 21:46 ? 00:00:01 (squid) -D -YC
proxy 4636 4634 0 21:46 ? 00:00:00 /usr/bin/perl /etc/webmin/squid/
squid-auth.pl /etc/webmin/squid/users
proxy 4637 4634 0 21:46 ? 00:00:00 /usr/bin/perl /etc/webmin/squid/
squid-auth.pl /etc/webmin/squid/users
proxy 4638 4634 0 21:46 ? 00:00:00 /usr/bin/perl /etc/webmin/squid/
squid-auth.pl /etc/webmin/squid/users
proxy 4639 4634 0 21:46 ? 00:00:00 /usr/bin/perl /etc/webmin/squid/
squid-auth.pl /etc/webmin/squid/users
proxy 4640 4634 0 21:46 ? 00:00:00 /usr/bin/perl /etc/webmin/squid/
squid-auth.pl /etc/webmin/squid/users
root 4789 4774 0 23:48 pts/1 00:00:00 grep squid
guide:~#

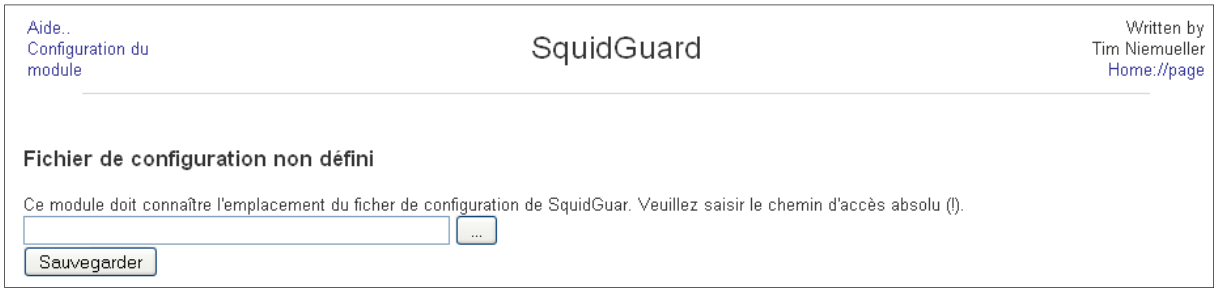
- Vérifier que le port d'écoute est correct.

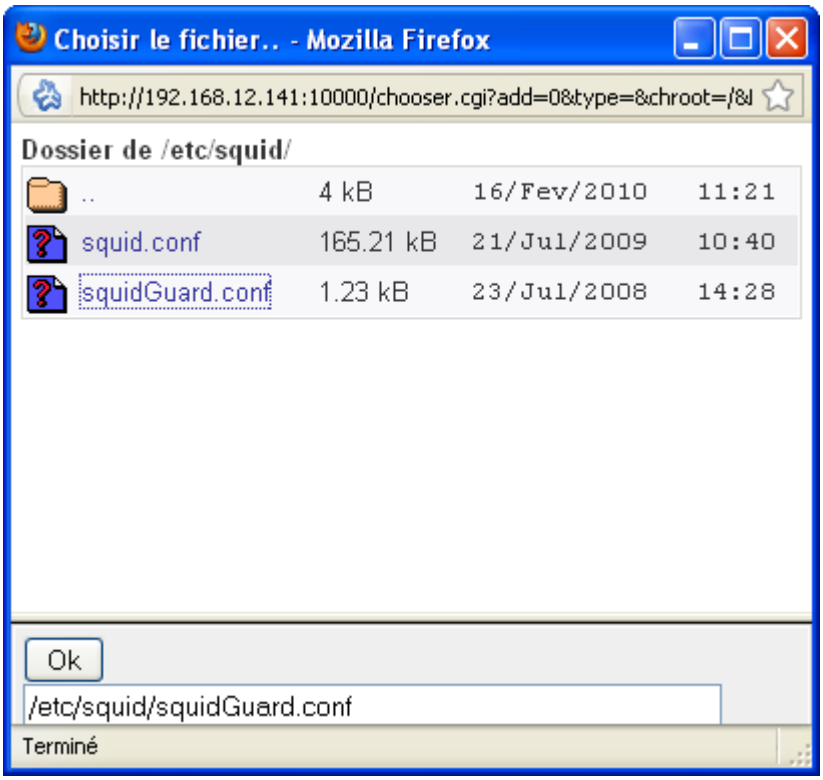
```
guide:~# netstat -avp | grep LISTEN
```

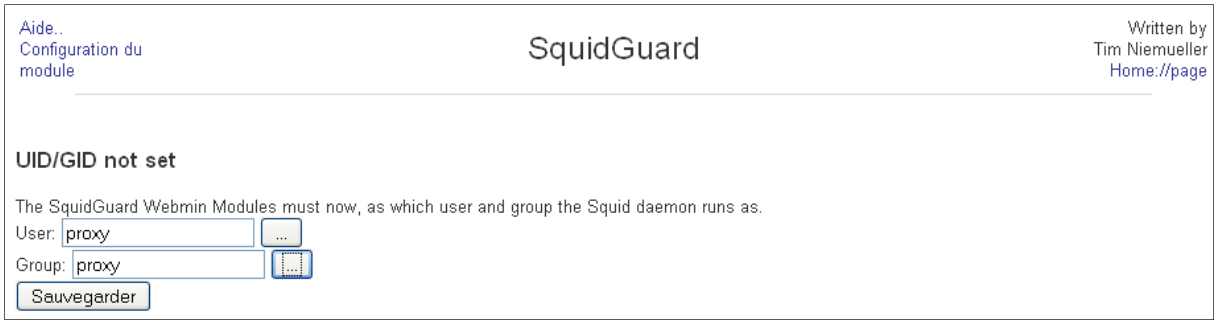
```
tcp        0      0 192.168.12.145:3128     *:*                     LISTEN
4634/(squid)
```

b. SquidGuard

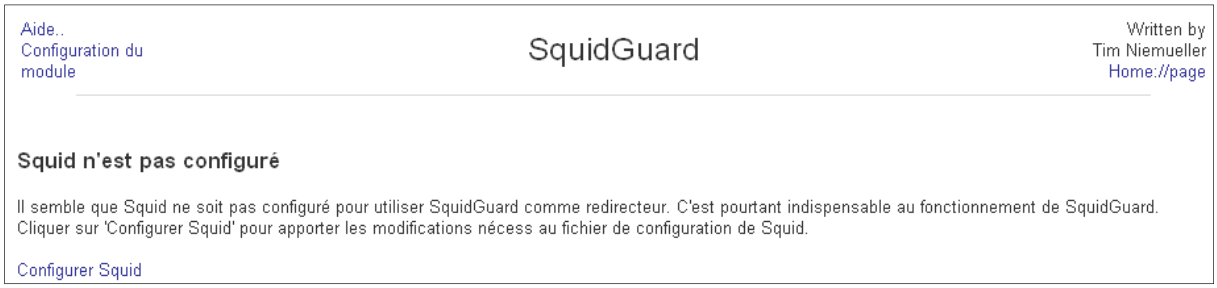
- Ouvrez l'onglet «serveurs» de l'interface webmin et cliquer sur l'icône «squidguard». Vous êtes invités à créer les chemins de: fichier de configuration, répertoires de la base et des journaux.







- A ce stade, Squidguard est configuré mais n'est pas encore opérationnel tant que Squid n'est pas encore informé de sa présence. Alors cette fenêtre vous invite à configurer squid.

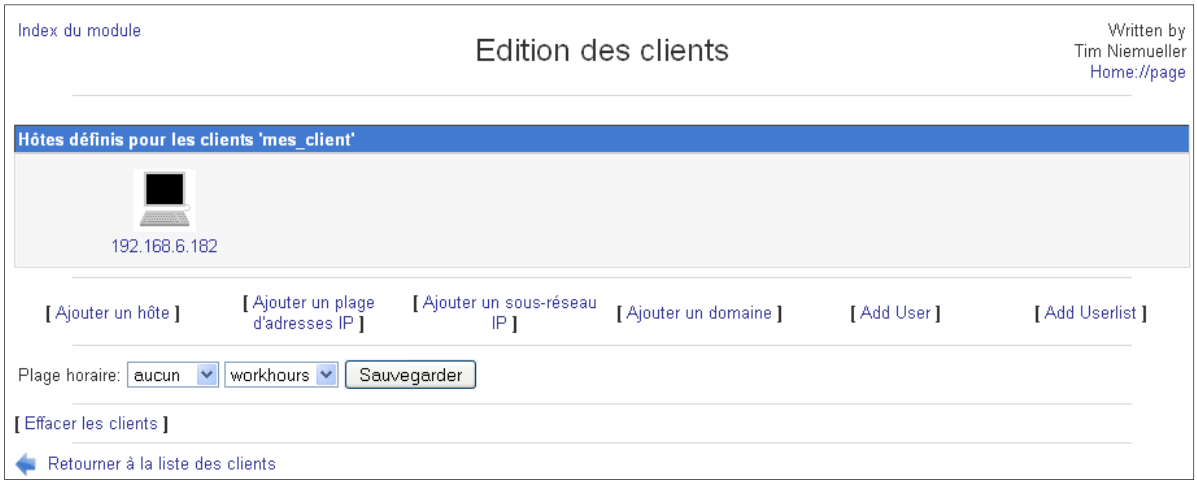

Aide..
Configuration du module
SquidGuard
Written by
Tim Niemueller
Home://page
Squid n'est pas configuré
Il semble que Squid ne soit pas configuré pour utiliser SquidGuard comme redirecteur. C'est pourtant indispensable au fonctionnement de SquidGuard.
Cliquer sur 'Configurer Squid' pour apporter les modifications nécess au fichier de configuration de Squid.
Configurer Squid

- Vous devriez avoir ceci dans la fenêtre Squidguard de Webmin

- **Ajout des clients :**

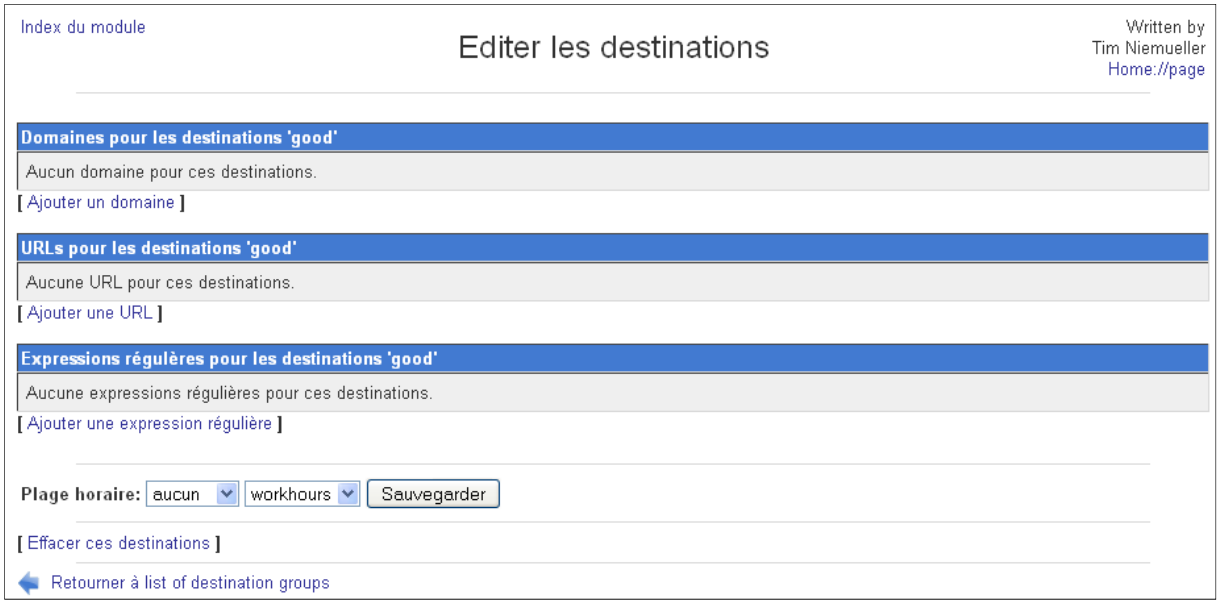
- Vous pouvez ajouter vos clients en cliquant sur l'icône « client », faites saisir le nom du groupe client et cliquez sur « Ajouter des nouveaux clients ».

- Editez le groupe de clients que vous venez de créer, comme ci-dessous il vous permet de créer les utilisateurs selon l'adresse de leur machine, leur plage d'adresse, leur nom… pour cet exemple j'ai ajouté une adresse hôte.


Index du module
Edition des clients
Written by
Tim Niemueller
Home://page
Hôtes définis pour les clients 'mes_client'
192.168.6.182
[Ajouter un hôte]
[Ajouter un plage d'adresses IP]
[Ajouter un sous-réseau IP]
[Ajouter un domaine]
[Add User]
[Add Userlist]
Plage horaire: aucun workhours Sauvegarder
[Effacer les clients]
Retourner à la liste des clients

- **Ajout de destination :**

- Le groupe « good » pour le réseau externe et le groupe « local » pour le réseau intene. Vous pouvez donc éditez un groupe et ajouter un nom de domaine ou **un** URL.

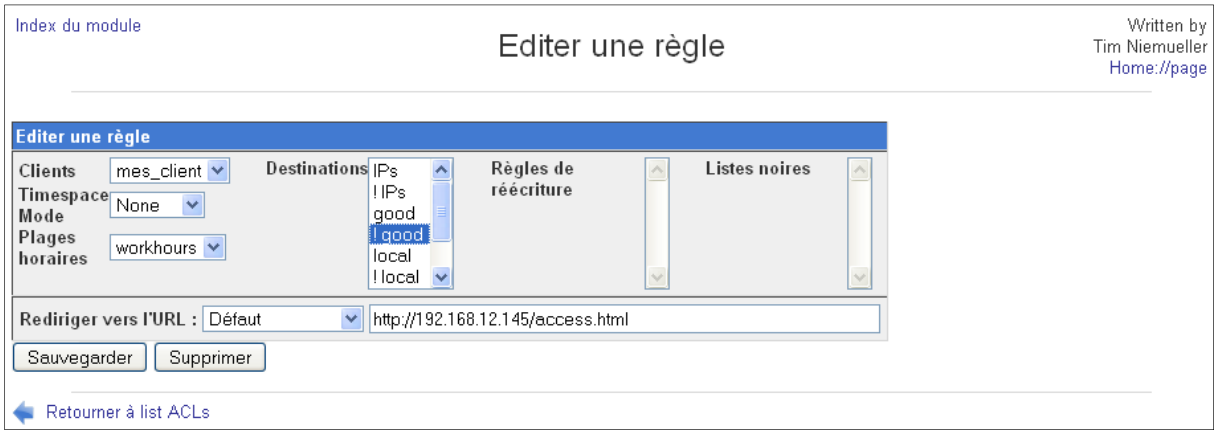

Index du module
Editer les destinations
Written by
Tim Niemueller
Home://page
Domaines pour les destinations 'good'
Aucun domaine pour ces destinations.
[Ajouter un domaine]
URLs pour les destinations 'good'
Aucune URL pour ces destinations.
[Ajouter une URL]
Expressions régulières pour les destinations 'good'
Aucune expressions régulières pour ces destinations.
[Ajouter une expression régulière]
Plage horaire: aucun workhours Sauvegarder
[Effacer ces destinations]
Retourner à list of destination groups

- **Listes de contrôle d'accès :**

Squidguard redirige les URLs interdits vers un URL local. Généralement, il s'agit d'un script CGI.

- Si cet URL de redirection n'est pas indiqué, Squidguard ne sache pas où rediriger les requêtes interdites, alors il les laissera passer.
- Il est donc impératif d'installer un tel script ou une page d'avertissement quelconque vers laquelle rediriger les URLs interdits en spécifiant son chemin dans l'ACL « default ».
- Cliquez sur « Listes de contrôle d'accès », spécifiez les clients puis cliquez sur « Ajouter une règle ».

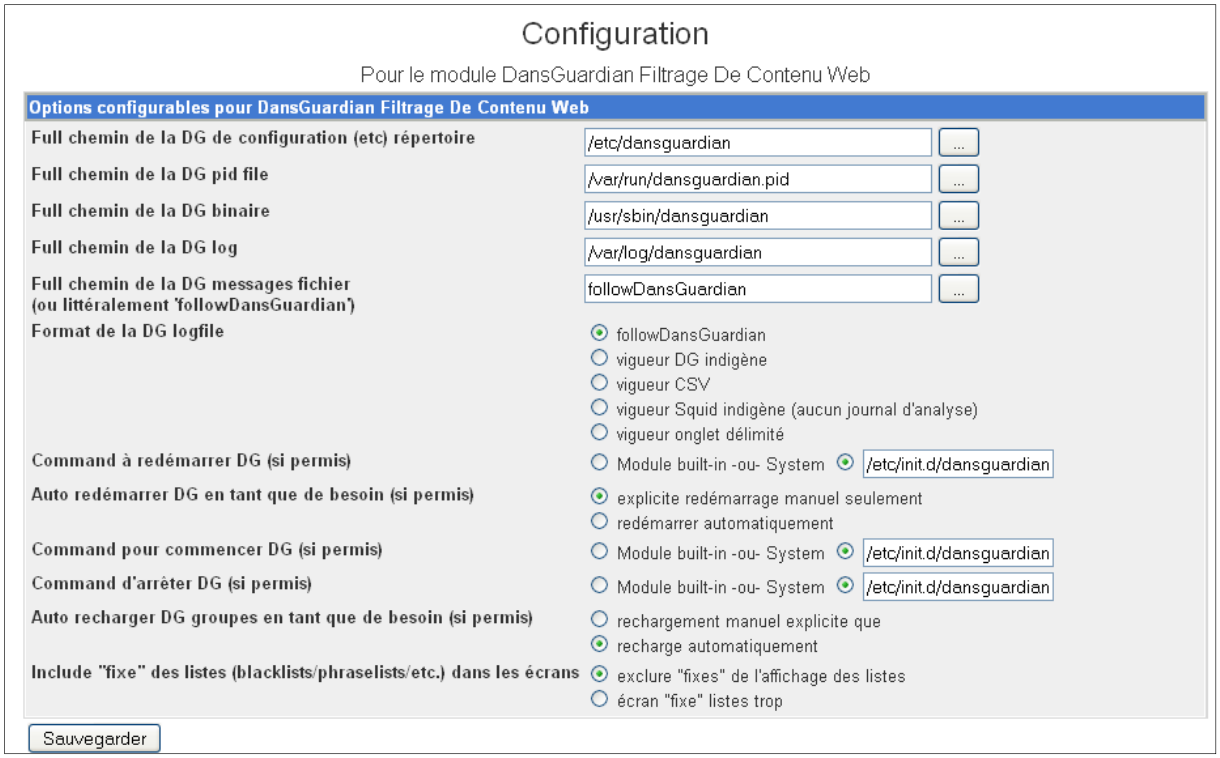
- Dans cet exemple, j'ai ajouté une règle qui redirige toutes connexions, où la destination n'est pas configurée dans la liste des URLs « good », vers une page interne.



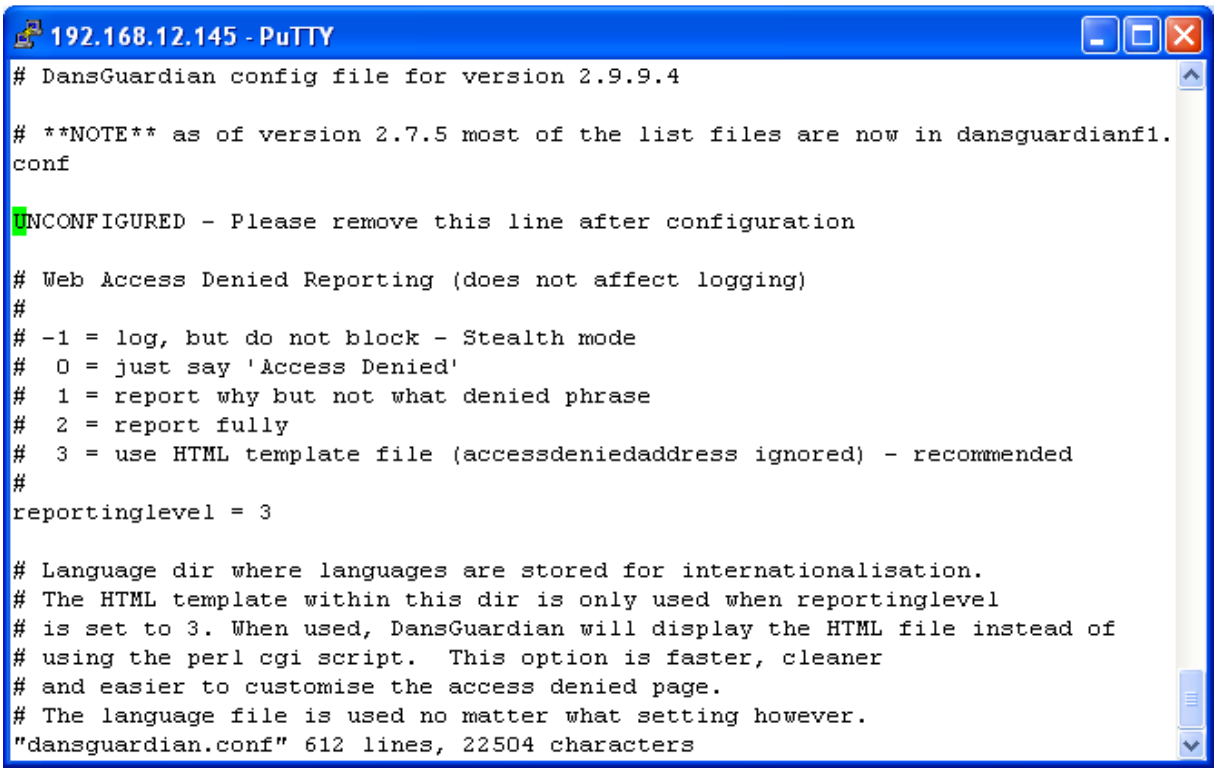
c. DansGuardian

- Sous la catégorie serveur, cliquez sur « DansGuardian filtrage de contenu web », cliquez sur configuration du module pour vérifier les chemins du répertoire de configuration, du log et du binaire. Puis sauvegardez.

Aide..
Configuration du module
DansGuardian
Version ? (Version du Module 0.7.0beta1b)
Démarrer DG
Rechercher la documentation..
DansGuardian - le filtrage de contenu web pour tous
Attention - dansguardian ne trouve pas de fichier binaire, vous avez peut-être besoin de mettre à jour votre Configuration du module (en particulier les chemins.)
(Chemin d'accès au fichier:: /sbin/dansguardian)
Attention - la version de dansguardian vous avez n'est pas supporté par ce module Webmin version
Version du Module 0.7.0beta1b DG soutient version 2.9/2.10
actuellement installés DG version ?
Attention - courir en tant que root (superles risques de nouveaux fichiers ne sont pas lisibles par la production dansguardian)


Configuration
Pour le module DansGuardian Filtrage De Contenu Web
Options configurables pour DansGuardian Filtrage De Contenu Web
Full chemin de la DG de configuration (etc) répertoire
/etc/dansguardian
Full chemin de la DG pid file
/var/run/dansguardian.pid
Full chemin de la DG binaire
/usr/sbin/dansguardian
Full chemin de la DG log
/var/log/dansguardian
Full chemin de la DG messages fichier (ou littéralement 'followDansGuardian')
followDansGuardian
Format de la DG logfile
followDansGuardian
vigueur DG indigène
vigueur CSV
vigueur Squid indigène (aucun journal d'analyse)
vigueur onglet délimité
Command à redémarrer DG (si permis)
Module built-in -ou- System
/etc/init.d/dansguardian
Auto redémarrer DG en tant que de besoin (si permis)
explicite redémarrage manuel seulement
redémarrer automatiquement
Command pour commencer DG (si permis)
Module built-in -ou- System
/etc/init.d/dansguardian
Command d'arrêter DG (si permis)
Module built-in -ou- System
/etc/init.d/dansguardian
Auto recharger DG groupes en tant que de besoin (si permis)
rechargement manuel explicite que
recharge automatiquement
Include "fixe" des listes (blacklists/phraselists/etc.) dans les écrans
exclure "fixes" de l'affichage des listes
écran "fixe" listes trop
Sauvegarder

- Editez le fichier «/etc/dansguardian/dansguardian.conf» et commentez ou supprimez la ligne « UNCONFIGURED ».

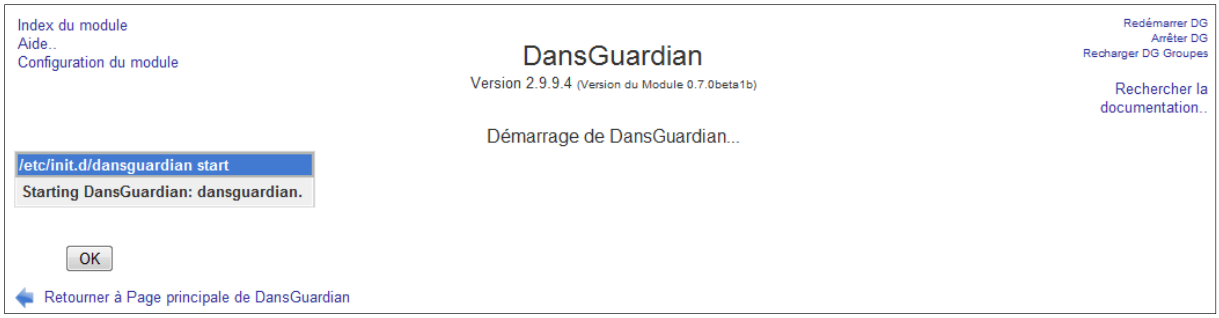

192.168.12.145 - PuTTY
DansGuardian config file for version 2.9.9.4
NOTE as of version 2.7.5 most of the list files are now in dansguardianf1.conf
UNCONFIGURED - Please remove this line after configuration
# Web Access Denied Reporting (does not affect logging)
# -1 = log, but do not block - Stealth mode
# 0 = just say 'Access Denied'
# 1 = report why but not what denied phrase
# 2 = report fully
# 3 = use HTML template file (accessdeniedaddress ignored) - recommended
reportinglevel = 3
# Language dir where languages are stored for internationalisation.
# The HTML template within this dir is only used when reportinglevel
# is set to 3. When used, DansGuardian will display the HTML file instead of
# using the perl cgi script. This option is faster, cleaner
# and easier to customise the access denied page.
# The language file is used no matter what setting however.
"dansguardian.conf" 612 lines, 22504 characters

- Retournez vers la page principale de DansGuardian d'index et cliquez sur « Voir et modifier la configuration ».

- Faire vérifier le port d'écoute de DansGuardian, ainsi que l'IP et le port du proxy squid. Puis cliquez sur le bouton « mise à jour ».

Aide..
Configuration du module
DansGuardian
Version 2.9.9.4 (Version du Module 0.7.0beta1b)
Démarrer DG
Rechercher la documentation..
DansGuardian - le filtrage de contenu web pour tous
Attention - courir en tant que root (superles risques de nouveaux fichiers ne sont pas lisibles par la production dansguardian)
STATUS
Afficher le statut de DansGuardian
ANALYZE
Consulter les logs de DG
SEARCH
Recherche de mots pour mots (ou de domaine ou URL)
SYSCONF
Voir/Modifier la configuration
PLUGINS
Voir/Modifier la Plugin configuration
SYSLISTS
Voir/Modifier les fichiers
XLATE
Voir/Modifier les messages système (traduction)
ASSIGN
Voir/Modifier groupe de filtrage Assignments
CONFS
Voir/Modifier Un filtre du Groupe de la Base de Config
LISTS
Voir/Modifier Un filtre du Groupe Lists)
MULTI
Voir Comment Listes et Configs Pour filtres multiples groupes sont constitués
SETUP
Set Up Listes & Configs Pour les filtres multiples Groupes

- Redémarrer Squid, ensuite Démarrer DansGuardian.



d. Mise à jour de Dansguardian

Certains sites non autorisés auront tendance à disparaitre de la toile avec l'apparition de nouveaux. De même, des phrases interdites pourraient devenir obsolète avec l'apparition de nouvelles inconnues dans la base de connaissance de Dansguardian.

Il est donc utile de maintenir la blacklist et la phraselist à jour. Vous pouvez vous rendre sur le site http://URLBlacklist.com pour télécharger la dernière mise à jour de la blacklist.

Enregistrez-la dans votre répertoire personnel et ensuite décompressez-la dans le répertoire /etc/dansguardian par :

```
# tar –xzvf  bigblacklist.tar.gz
```

De même pour la mise à jour de phraselist http://contentfilter.futuragts.com/phraselists/

Maintenant vous pouvez configurer la blacklist de votre dansguardian :

- L'autorisation d'accès à vos sites se trouve dans le fichier /etc/dansguardian/exceptionsitelist
- A l'inverse, /etc/dansguardian/bannedsitelist gère les sites non autorisés (vous pouvez tester avec badboys.com qui est l'exemple par défaut de ce fichier et dansguardian vous en refusera l'accès).
- Bloquer tout sites contenant une phrase se trouvant dans le fichier /etc/dansguardian/bannedphraselist.
- Autoriser des phrases dans le contenu d'un site dans le fichier /etc/dansguardian/exception phraselist.

N.B : le site URLBlacklist.com est un site payant qui ne permet qu'un et un seul téléchargement gratuit de la blacklist. Il vous faudra ensuite, pour maintenir votre blacklist à jour, soit souscrire à un abonnement, soit trouver un site qui fournisse ce service gratuitement.

e. Configuration du client

Configurez le client pour qu'il utilise le service proxy sur les requêtes HTTP. Donc sous l'onglet outils du navigateur cliquez sur « options internet/connexions/paramètres réseau. Puis cochez le serveur proxy et faites entrer l'adresse et le port de l'écoute de Dansguardian.

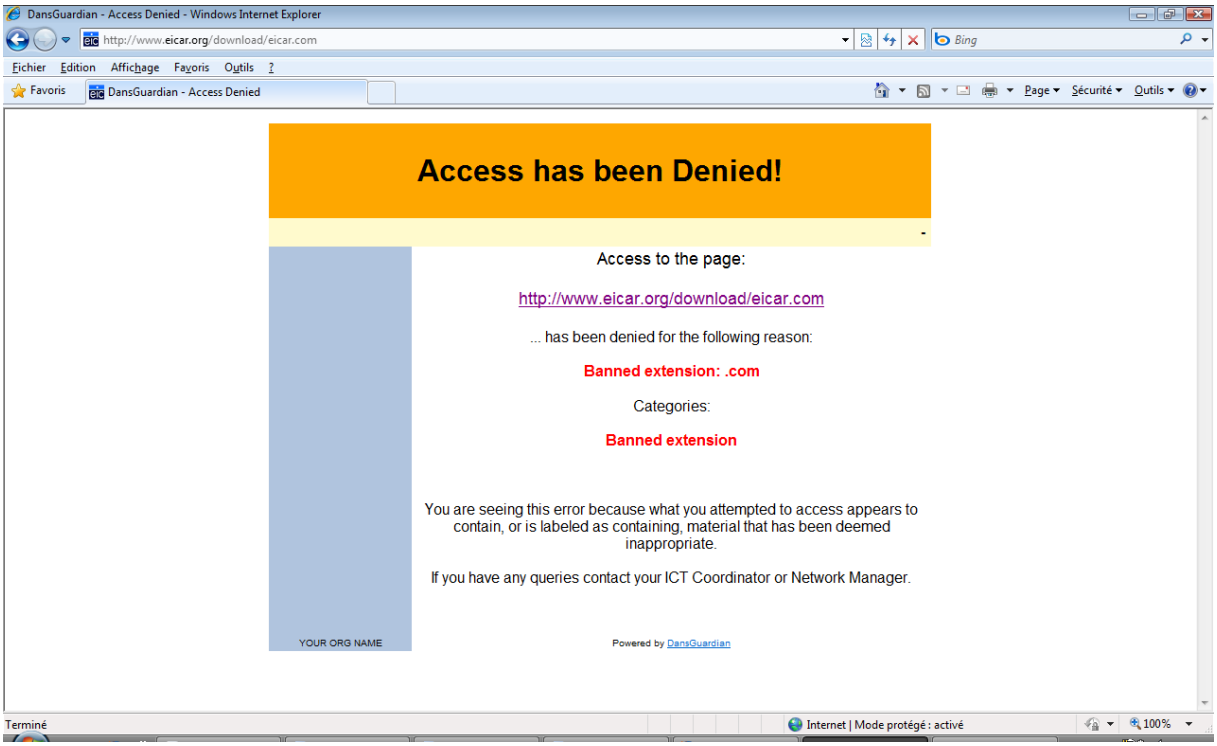
Options Internet
Paramètres du réseau local
Configuration automatique
La configuration automatique peut annuler les paramètres manuels. Pour garantir leur utilisation, désactivez la configuration automatique.
Détecter automatiquement les paramètres de connexion
Utiliser un script de configuration automatique
Adresse
Serveur proxy
Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliquent pas aux connexions d'accès à distance ou VPN).
Adresse : 42.168.216.133
Port : 8080
Avancé
Ne pas utiliser de serveur proxy pour les adresses locales
OK
Annuler
Paramètres du réseau local
Les paramètres du réseau local ne s'appliquent pas aux connexions d'accès à distance. Cliquez sur le bouton Paramètres ci-dessus pour définir les options de numérotation.
Paramètres réseau
OK
Annuler

5. TEST DE FONCTIONNEMENT

Ouvrez maintenant votre navigateur et rendez-vous sur ce site, qui implémente plusieurs types de fichiers contenant le "virus de test" EICAR, afin de tester le filtre Dansguardian:

http://www.eicar.org/download/eicar.com

Cette page doit être refusée !


DansGuardian - Access Denied - Windows Internet Explorer
http://www.eicar.org/download/eicar.com
Fichier Edition Affichage Favoris Outils ?
Favoris
DansGuardian - Access Denied
Page Sécurité Outils
Access has been Denied!
Access to the page:
http://www.eicar.org/download/eicar.com
... has been denied for the following reason:
Banned extension: .com
Categories:
Banned extension
You are seeing this error because what you attempted to access appears to contain, or is labeled as containing, material that has been deemed inappropriate.
If you have any queries contact your ICT Coordinator or Network Manager.
YOUR ORG NAME
Powered by DansGuardian
Terminé
Internet | Mode protégé : activé
100%

N.B :

1) Il se peut que DansGuardian génère des faux-positifs en refusant l'accès à des pages telles que google. L'autorisation d'accès à vos sites se trouve dans le fichier /etc/dansguardian/exceptionsitelist. A l'inverse, /etc/dansguardian/bannedsitelist gère les sites non autorisés.
2) N'oubliez pas de relancer DansGuardian à chaque modification des listes.